REMARKS

The Office Action dated March 6, 2008, has been received and carefully considered. Claim 1 has been amended to more carefully recite the subject matter. Claim 2 has been cancelled without prejudice or disclaimer to the subject matter contained therein. No new matter has been added. Reconsideration of the pending rejections in the present application is respectfully requested based on the following remarks.[1]

I. CLAIM REJECTIONS 1-20 UNDER 35 U.S.C. 103(a)

On pages 3-9 of the Office Action, claims 1-20 were rejected under 35 U.S.C. § 103(a) as being anticipated by Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

[1] As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41..

Regarding claim 1, the Examiner asserts that Rogaway discloses certain aspects of the claimed invention. Applicant

respectfully disagrees. The Examiner has broadly interpreted some aspects of the claims in a manner that Applicant disagrees with. For example, page 5 of the Office Action interprets the claimed "first mask value" and "second mask value" as being identical. Indeed, the Examiner relies on this interpretation in applying Rogaway to portions of the claim. Applicant disagrees with this interpretation, and would like to respectfully point out that such an interpretation is no longer tenable based upon the amendment to the claims in the January 7, 2008 communication. However, in the interest of forwarding this application towards allowance, Applicant has amended independent claim 1 to preclude this interpretation.

Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method comprising:

> whitening at least one message block with a *first mask value*;
> encrypting the at least one whitened message block using a block cipher and a first key; and
> whitening the at least one encrypted message block with a *second mask value*, which is not identical to the first mask value, to generate at least one corresponding output ciphertext block;
> wherein the *first mask value* is computed by applying a XOR function to a first value derived from a NONCE value and a second value derived from encrypting a third value using the block cipher and a second key,

> and then applying a substitution function to the result of the XOR function;
>
> wherein the first and second key have different values;
>
> wherein the *second mask value* is computed by applying a XOR function to a fourth value derived from the NONCE value and a fifth value derived from encrypting a sixth value using the block cipher and the second key, and then applying the substitution function to the result of the XOR function. (emphasis added)

Applicant respectfully submits that Rogaway fails to teach, or even suggest a first mask value or a second mask value as recited in independent claim 1. The generated value in the Rogaway XOR operations alleged by the Examiner to be equivalent to the two claimed whitening operations is the same in both operations. This is quite different from a first mask value and a second mask value that are not identical in value as recited in claim 1.

Further, Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method that includes, *inter alia*, two keys having different values from each other, as presently claimed. In contrast, Rogaway explicitly discloses using a single key (see Rogaway, pg. 8: "One needs a single key, K, which keys all invocations of the underlying block cipher."). Additionally, the Examiner acknowledges the Rogaway deficiency

(see Office Action, pg. 7: "Rogaway does not specify that the key used to encrypt the value to generate the 'L' (page 5) is different than the key used to encrypt M[i] ⊕ Z[i] (page 5)."). Schneier does not cure these deficiences. Indeed, this is not even alleged. Accordingly, is it respectfully submitted that claim 1 is allowable over the combination of Rogaway and Schneier.

It would not have been obvious to one reasonably skilled in the art to modify Rogaway to arrive at the claimed invention. Rogaway is sufficiently different from the method as recited in claim 1 such that it would not have been obvious to modify Rogaway. The claim recites multiple keys. Rogaway describes the use of a single key. The claim recites that the multiple keys have different values. Rogaway only recites the use of a single key. Thus, even if that key was used multiple times, it is substantially different than the claim because it explicitly recites using a single key value.

Any proposed modification to Rogaway would render the teachings of Rogaway unsatisfactory for its intended purpose. As stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900,

221 USPQ 1125 (Fed. Cir. 1984). Further, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

A modification to Rogaway that arrives at the claimed invention in turn renders Rogaway unsatisfactory for its intended purpose. The Rogaway system calls for modest memory requirements and limited pre-processing capability (see Rogaway, pg. 8). The reference explicitly discloses that the memory requirements and pre-processing capability are only expanded for limited purposes, such as storing L(i) values. In this discussion, reference is made to the single key (K). There is no teaching of flexibility with respect to K. Rather, Rogaway reiterates that the key is a single value. Accordingly, any modification away from that single value key frustrates the intended purpose of having the most efficient possible system with modest memory requirements and limited processing capability.

For at least these reasons, claim 1 is nonobvious over the cited references. Claims 3-11 are allowable because they are dependent on claim 1 and thus inherently incorporate all of the

limitations of independent claim 1. Also, the secondary reference (i.e., Schneier) fails to disclose, or even suggest the deficiencies of the primary reference as discussed above with respect to claim 1. Accordingly, claims 3-11 are allowable over the combination of the secondary reference with the primary reference at least by virtue of their dependency on independent claim 1. Moreover, claims 3-11 recite additional features which are not disclosed or suggested by the cited references when taken alone or in combination.

Regarding claim 12, the Examiner asserts that the claimed invention would have been obvious in view of the combination of Rogaway and Schneier. Applicant respectfully disagrees. The Examiner (see Office Action, pg. 3) alleges that the Rogaway disclosure of concatenating message blocks meets the recited claim 12 element of applying an XOR function to all message blocks of a message to compute an XOR-sum. The Examiner states "concatenation effectively creates the XOR-sum." Applicant disagrees that the concatenation described in Rogaway meets this claim element. A concatenation operation is very different from an XOR operation in both form and result. Applicant respectfully requests withdrawal of the rejection.

Furthermore, Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block

cipher E_k, as well as applying the same message string M[m] after the block cipher E_k (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally, Rogaway also discloses applying an offset Z[m] to a checksum before a block cipher E_k, and then limiting the block cipher result to a tag length τ (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Regarding combining Schneier with Rogaway to arrive at the claimed invention, such a combination would result in an inoperable methodology since replacing the result of encrypting of Rogaway with an additional XOR function as mentioned by Schneier would not result in a limited tag length τ, which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 12 is allowable over the combination of Rogaway and Schneier.

Regarding claims 13-20, these claims are dependent upon independent claim 12. Thus, since independent claim 12 should be allowable as discussed above, claims 13-20 should also be allowable at least by virtue of their dependency on independent claim 12. Moreover, these claims recite additional features

which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

At this point Applicant would like to respectfully note that, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Also, as stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 3-7, 10, and 12-20 be withdrawn.

II. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

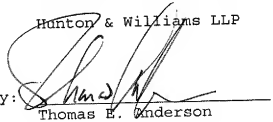
To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

Date: June 3, 2008

By: 

Thomas E. Anderson
Registration No. 37,063

TEA/ple

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201